1. Cos'è l'hacking?

L'hacking è l'insieme dei modi non convenzionali per interagire con i sistemi, queste interazioni sono al di fuori delle intenzioni degli sviluppatori del software, hardware, o del sistema di rete.

In breve con il termine hacking ci si riferisce all'utilizzo di un sito web, un sistema, o una API in un modo per cui esso non è stato progettato, cercando di estenderne l'utilizzo.

Chi è l'hacker?

Il termine hacker designa una persona che trae piacere nell'esplorare i dettagli nei sistemi programmabili e sperimenta come *estenderne l'utilizzo*.

I diversi tipi di hacker:

- Black hat
  - Hacker 'Cattivo': è un hacker malintenzionato o con intenti criminali, mantiene segrete le proprie conoscenze sulle vulnerabilità e gli exploit[1].
- White hat (Ethical hacker)
  - Hacker 'Bravo': è un hacker che attacca solo con autorizzazione (penetration testing) e si contrappone a chi viola illegalmente sistemi informatici.
- Grey hat
  - Combinazione di Black hat e White hat.
- Suicide Hacker
  - Non si interessano delle conseguenze, come andare dietro le sbarre. (es. Julian Assange)
- Script Kiddies
  - Usano i strumenti (tools) senza comprenderne il funzionamento
- Cyber Terrorista
  - Creano caos/paura distruggendo infrastrutture critiche
- Hacker di stato
  - Assunti dai governi

[1] Exploit: tradotto "sfruttare", identifica una tipologia di script, virus, worm, porzione di dati o binario che sfrutta un bug o una vulnerabilità per creare comportamenti non previsti in software, hardware, o in sistemi elettronici

- Hacktivisti
  - Motivati da ideologie politiche, sono il mix tra hacking e attivismo (es. Anonymous)

Livelli di abilità:

Script kiddies: Chi utilizza solamente strumenti di exploit, script e programmi già costruiti per poter condurre attacchi senza comprendere realmente come l'attacco funziona.

Tecnici: Chi utilizza sia soluzioni già esistenti sia soluzioni personalizzate. Un tecnico può capire come un attacco funziona utilizzando uno strumento già esistente che potrebbe però non funzionare ma adattarlo per poter portare a successo l'exploit.

Guru: Rappresentano l'1337[2]. Sviluppano i loro strumenti, e capiscono fino in fondo i sistemi, le comunicazioni di rete, il livello basso dei sistemi operativi, la programmazione l'assembly, ecc.

[2] Il **leet** (o anche **l33t**, **31337** o **1337**) ha origine dalla parola "élite", in inglese si pronuncia simile a "leet", è usato anche come sinonimo di bravura fuori dall'ordinario, nell'ambito dei videogiochi online e dell'hacking.

Perchè le persone hackerano?

Nel senso più ampio le ragioni che portano gli hacker a fare ciò che fanno sono 4:

- Acquisire dati
- Impersonificare
- Distruggere
- Soldi
- *Divertirsi*
- **Altri fattori**
    - Fornitura illimitata: pensando ad un server, questo è costantemente in rete per poter essere raggiunto da tutti, poterlo hackerare può aprire ad una vastità di motivi, come il defacing oppure la possibilità di utilizzarlo a proprio piacimento.
    - Facilità d'attacco: spesso risulta molto semplice effettuare un attacco.
    - Immaturità del settore: nonostante la sua importanza, si da poco peso all'importanza che la sicurezza informatica rappresenta.
    - Anonimato: la vastità di tecnologie che consentono di acquisire facilmente un buon grado di anonimato (es. Tor Browser), consentono di sferrare straordinari attacchi senza essere scoperti.

2. Metodi di attacco

Concettualmente gli attacchi si possono raggruppare in 3 categorie:

1. Fisico
    - Entrare dentro un edificio, prendere un computer e andarsene
2. Digitale
    - Metodi di “Hacking” tradizionale, attacchi di rete, ecc.
3. Sociale
    - Ingegneria sociale. Impersonificare o suscitare le persone a fornire informazioni sensibili attraverso l'interazione sociale

3. Penetration Testing

Negli ultimi anni, la popolarità del penetration testing è significativamente accresciuta e ormai è diventato un metodo mainstream per poter mantenere l'integrità dal punto di vista della sicurezza.

Cos'è il penetration testing?

- ❖ Penetration testing (o brevemente pentesting) è un attacco simulato e autorizzato ad un sistema di computer o ad una rete per poter valutare la sua sicurezza.

Che beneficio ottiene un'azienda dal penetration testing?

- ❖ Tradizionalmente la "sicurezza difensiva" mirava a soluzioni reattive come patchare e rivedere la configurazione.
  La sicurezza offensiva invece si focalizza su essere proattivi e tentare di identificare e fare leva sulle esistenti falle di sicurezza mentre si provvede ad un report riguardante i rischi dell'azienda e l'importanza dei problemi di sicurezza rilevati.

Esistono quattro diverse categorie di pentesting:

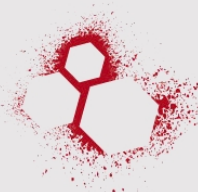
- Vulnerability Assessment
- Penetration Testing
  - White box
  - Black box
  - Grey box

Il Vulnerability Assessment (VA) è un processo che consiste nell'individuare, quantificare e prioritizzare le vulnerabilità, essenzialmente viene effettuato un vulnerability scan attraverso uno o la combinazione di molteplici strumenti disponibili, spesso a pagamento, generando un report che sarà poi valutato da esperti, pertanto eseguire solo un VA non può essere considerato un vero e

proprio pentesting, tuttavia prima di un'attività di penetration testing è inevitabile effettuare un Vulnerability Assessment, per poter consentire di individuare molto più facilmente eventuali vulnerabilità.

Le valutazioni(assessments) vengono in genere eseguite in base ai seguenti passaggi:

1. Catalogazione di risorse e capacità in un sistema.
2. Assegnazione di valore quantificabile e importanza a tali risorse
3. Identificazione delle vulnerabilità o potenziali minacce a ciascuna risorsa
4. Mitigare o eliminare le vulnerabilità più gravi per le risorse più preziose

   I strumenti (Vulnerability scanner) più utilizzati, gratuiti e a pagamento, sono i seguenti:

Nikto 2

Il primo(Nmap) non è un vero e proprio vulnerability scanner tuttavia risulta essere comunque utile nell'individuazione di vulnerabilità.
Nmap (acronimo di Network mapper), è un tool che consente di effettuare port scanning ovvero di poter individuare le porte aperte, chiuse o filtrate.
In realtà però dalla sua creazione (1 settembre 1997) è diventato uno strumento indispensabile per ogni amministratore di sistema, perché è in grado oltre ad eseguire un semplice scan delle porte, di ipotizzare il sistema operativo utilizzato e le versioni dei servizi in uso, è estremamente versatile e rende facile anche la scansione di un'intera rete.
Grazie agli script NSE (Nmap Scripting Engine, https://nmap.org/man/it/man-nmap-scripting-engine.html) che estendono l'uso di nmap, è possibile effettuare seppur limitatamente un vulnerability scan.

Il Penetration Testing (PT) è volto a dimostrare l'efficacia di un Vulnerability Assessment effettuando la simulazione di un attacco reale, come abbiamo visto può essere di tre tipi, *white box*, *black box* e *grey box*.

Con il *white box* si ha a disposizione l'applicazione con il relativo codice sorgente e l'ambiente di sviluppo oltre che la possibilità di fare ciò che si vuole e di interagire con il client.

A differenza del *white box* per cui si ha a disposizione il codice, con il *black box* non è noto a priori né il codice sorgente né come si comporta, l'unico modo di studiarne il comportamento sta nelle risposte di output.

Come è facilmente intuibile il metodo *grey box* rappresenta il mix tra *black box* e *white box*.

Tipi di penetration test:

- Web Application
  - Riferito ad attacchi a siti web e genericamente a tutte le applicazioni distribuite web-based.
- Web Services
  - Sostanzialmente si riferisce ad attacchi alle API[3].
- Social Engineering
  - Studio del comportamento individuale di una persona al fine di carpire informazioni utili.
- Wireless
  - Attacchi riferiti alle reti Wi-Fi
- Application
  - Attacchi riferiti alle applicazioni
- External
  - Altre tipologie (es. attacchi alla VPN, Web Mail, ecc.)
- Mobile
  - Attacchi a dispositivi e applicazioni mobile
- Internal/Infrastructure

[3] **Application Programming Interface**[1] (**API**) si indica un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito.

- ➢ Attacchi alla rete interna (enumerazioni dispositivi, controllo del traffico, ecc.)
- ❖ SCADA
  - ➢ Attacco alla supervisione di sistemi fisici (l'automazione industriale)
- ❖ Client-side
  - ➢ Attacchi livello client
- ❖ Red Team
  - ➢ Riguarda tutto, dal normale hacking digitale, all'invio di email di phishing, fino al social engineering, basta trovare un modo di 'bucare' l'azienda, ovviamente con le autorizzazioni necessarie.

Per eseguire un degno penetration test è necessario seguire dei tipici step:

1. Raccolta di informazioni (footprinting)
   - ★ Come un ladro che cerca di svaligiare una banca, prima di entrare e chiedere i soldi, si preoccupano di raccogliere più informazioni possibili sul target, al termine di questa fase l'hacker ha a disposizione un *footprint*, ovvero un profilo univoco del bersaglio.
2. Scansione
   - ★ Se il footprinting è utile ad inquadrare il bersaglio, come avere a disposizione una mappa, la scansione è come andare alla ricerca di *porte* e finestre.
     - A. Si determina se il sistema è attivo
     - B. Si determinano il tipo di sistema e i servizi in esecuzione (o ascolto)
     - C. Si salvano i risultati ottenuti
3. Enumerazione
   - ★ Una volta individuati gli host e i servizi attivi, si passa ad esaminarli in dettaglio cercandone i punti deboli, la differenza tra enumerazione e raccolta delle informazioni sta nel livello di intrusività.

A. Si effettua un fingerprinting dei servizi
B. Si effettua un vulnerability scan
C. Si effettua la cattura di banner
D. Si enumerano i servizi di rete comuni

4. Exploitation
   ★ Prendere il controllo di uno o più devices.

5. Post-exploitation
   ★ Mantenimento dell'accesso, carpire informazioni e muoversi nella rete target

6. Eliminare le tracce/Reporting